Infra-Estrutura de Chaves Públicas Brasileira

Manual de Condutas Técnicas 11 - Volume II

Procedimentos de Ensaios para Avaliação de Conformidade aos Requisitos Técnicos de Softwares de AC e AR no âmbito da ICP-Brasil

Versão 1.0

Sumário

Listas de Ilustrações

Lista de Figuras

Lista de Tabelas

Glossário

Os termos utilizados neste MCT se referem àqueles definidos no Glossário ICP-Brasil [08] conforme seção de referências normativas.

Lista de Acrônimos

AC	Autoridade Certificadora
AC Raiz	Autoridade Certificadora Raiz da ICP-Brasil
ANSI	*American National Standards Institute*
AR	Autoridade Registradora
BER	*Basic Encoding Rules*
CMS	*Cryptographic Message Syntax*
CRL	*Certificate Revocation List*
CSR	*Certificate Signing Request*
DER	*Distinguished Encoding Rules*
DPC	Declaração de Práticas de Certificação
HSM	*Hardware Security Module*
HTTP	*Hypertext Transfer Protocol*
ICP	Infra-Estrutura de Chaves Públicas
ICP-Brasil	Infra-Estrutura de Chaves Públicas Brasileira
IP	*Internet Protocol*
ITI	Instituto Nacional de Tecnologia da Informação
LCR	Lista de Certificados Revogados
LEA	Laboratório de Ensaios e Auditoria
MCT	Manual de Condutas Técnicas
MSC	Módulo de Segurança Criptográfico
NSH	Nível de Segurança de Homologação
OCSP	*Online Certificate Status Protocol*
OID	*Object Identifier*
PC	Políticas de Certificado
PEM	*Privacy Enhanced Mail*
PKCS	*Public-Key Cryptography Standards*
RFC	*Request For Comments*

1. Introdução

Este documento descreve os procedimentos de ensaio para homologação de software de AC e AR no âmbito da infra-estrutura de Chaves Públicas Brasileira, a ICP-Brasil.

Os procedimentos de homologação fazem referência ao conjunto de métodos que serão usados para avaliar se um software de AC e AR está ou não em conformidade com os requisitos técnicos definidos pelo “Manual de Condutas Técnicas 11 - Volume I”.

1.1 Organização deste documento

Cada seção deste documento contém um conjunto de requisitos que representam citações diretas do próprio texto do “Manual de Condutas Técnicas 11 - Volume I”. Os requisitos estão organizados da seguinte forma:

●REQUISITO <número_do_requisito>.<número_de_sequência_do_requisito>:

●“número_do_requisito”: corresponde ao número de área definido no Manual de Condutas Técnicas 11 – Volume I.

●“número_de_sequência_do_requisito”: corresponde a um identificador seqüencial dos requisitos.

Os procedimentos de homologação visam a orientar sobre como proceder nos ensaios para um software de AC e AR. Os procedimentos de ensaio estão classificados e agrupados por Níveis de Segurança de Homologação da seguinte forma:

●NSH 1: Este nível não requer depósito e análise de código-fonte associado ao software de AC e AR em homologação;

●NSH 2: Este nível requer depósito e análise apenas de código-fonte de componentes específicos associados ao software de AC e AR em homologação;

●NSH 3: Este nível requer depósito e análise de código-fonte completo associado ao software de AC e AR em homologação.

Os procedimentos de ensaio (EN) que devem ser desempenhados pelo analista LEA estão organizados da seguinte forma:

●EN.<número_do_requisito>.<número_de_sequência_do_requisito>.<número_de_sequência_do_ensaio>:

●“número_do_requisito”;

●“número_de_sequência_do_requisito”;

●“número_de_sequência_do_ensaio”: corresponde a um identificador seqüencial dos procedimentos que devem ser desempenhados.

Este documento (MCT 11 – Volume II) está estruturado da seguinte forma:

- Parte 1: Descreve os procedimentos de ensaio que devem ser verificados no processo de homologação de Softwares de AC e AR no âmbito da ICP-Brasil.

2. Parte 1

Procedimentos de ensaio para Homologação de Software de AC e AR no âmbito da ICP-Brasil

2.1 Requisitos aplicáveis somente ao Software de AC

Nesta seção estão definidos os requisitos aplicáveis apenas a um Software de AC.

2.1.1 Requisitos Gerais de um Software de AC

REQUISITO I.01: Um Software de AC deve oferecer todas as funcionalidades necessárias para o gerenciamento completo do ciclo de vida do certificado digital.

Procedimentos de ensaio para NSH 1, 2 e 3:

EN.I.01.01: Verificar se a documentação técnica do Software de AC inclui uma descrição do processo de gerenciamento do ciclo de vida do certificado digital, conforme item 2.1.1 do MCT 11 Vol. I.

EN.I.01.02: Realizar um ensaio prático acessando o software da AC e verificar se este oferece todas as funcionalidades necessárias para o gerenciamento completo do ciclo de vida do certificado digital. Para tal, verificar a disponibilidade de funcionalidades como solicitar, gerar e emitir um certificado digital, publicar o certificado digital, publicar uma LCR, revogar um certificado digital, renovar um certificado digital etc.

Procedimentos de ensaio para NSH 2 e 3:

EN.I.01.03: Verificar no código-fonte do Software de AC as rotinas para executar as funcionalidades necessárias para o gerenciamento completo do ciclo de vida do certificado digital. Depois, testar as execuções dessas rotinas.

RECOMENDAÇÃO I.01: Um software de AC pode suportar a funcionalidade de arquivamento e recuperação de par de chaves criptográficas assimétricas para certificados digitais ICP-Brasil de sigilo de usuários finais.

Procedimentos de ensaio para NSH 1, 2 e 3:

EN.REC.I.01.01: Verificar se a documentação técnica do Software de AC inclui:

- Uma afirmação da PI informando que não suporta esta recomendação; ou
- uma descrição do processo de arquivamento e recuperação de par de chaves criptográficas assimétricas para certificados digitais ICP-Brasil de sigilo de usuários finais.

EN.REC.I.01.02: Se o Software de AC suportar esta recomendação, realizar um ensaio prático acessando o software da AC, para arquivar e recuperar o par de chaves criptográficas assimétricas de um certificado digital ICP-Brasil de sigilo.

RECOMENDAÇÃO I.02: Um software de AC pode suportar o serviço de OCSP [14].

Procedimentos de ensaio para NSH 1, 2 e 3:

EN.REC.I.02.01: Verificar se a documentação técnica do Software de AC inclui:

- Uma afirmação da PI informando que não suporta esta recomendação; ou
- uma descrição da implementação do serviço de OCSP com as seguintes informações:
    - descrição da requisição OCSP com detalhes de parâmetros suportados;
    - descrição da resposta OCSP e a validação da mesma.

EN.REC.I.02.02: Se o Software de AC suportar esta recomendação, utilizando uma ferramenta desenvolvida pelo LEA, realizar requisições OCSP para um determinado certificado digital emitido e verificar se as respostas obtidas estão corretas.

REQUISITO I.02: Um Software de AC deve utilizar, no mínimo, os padrões e algoritmos criptográficos definidos pela ICP-Brasil conforme DOC-ICP-01.01 [4] para executar suas operações.

Procedimentos de ensaio para NSH 1, 2 e 3:

EN.I.02.01: Verificar se a documentação técnica do Software de AC inclui uma descrição dos padrões e algoritmos criptográficos utilizados pelo Software de AC.

EN.I.02.02: Verificar se esses padrões e algoritmos são, no mínimo, os definidos pela ICP-Brasil conforme DOC-ICP-01.01 [4].

Procedimentos de ensaio para NSH 2 e 3:

EN.I.02.03: Verificar no código-fonte do Software de AC se este contém rotinas para os padrões e algoritmos criptográficos definidos pela ICP-Brasil conforme DOC-ICP-01.01 [4] para executar suas operações.

2.1.2 Requisitos de Solicitação de Certificados Digitais

A solicitação de certificado digital pode ser feita diretamente na AC ou por meio de um intermediário na forma de uma AR utilizando um canal seguro. Na solicitação, o usuário final fornece os dados da CSR PKCS#10, os seus dados de titular e os dados do perfil do certificado digital desejado. Os dados de titular devem ser validados por um agente de registro que depois terá a responsabilidade de liberar ou negar a emissão do certificado digital.
A solicitação é recebida pelo Software de AC por meio de uma requisição formatada pela AR ou diretamente pelo usuário final por meio de uma interface que o Software de AC torna disponível.

REQUISITO I.03: Um Software de AC deve receber e validar uma requisição de certificado digital somente no formato CSR PKCS#10 [11] que contém a chave pública do usuário final.

Procedimentos de ensaio para NSH 1, 2 e 3:

EN.I.03.01: Verificar se a documentação técnica do Software de AC inclui uma descrição sobre os processos de recebimento e validação para uma requisição de

certificado digital. Verificar se esses processos estão somente no formato CSR PKCS#10 [11] que contém a chave pública do usuário final.

EN.I.03.02: Utilizando uma ferramenta desenvolvida pelo LEA, gerar uma requisição de um certificado digital no formato CSR PKCS#10 [11] e verificar se o Software de AC valida esta requisição.

EN.I.03.03: Utilizando uma ferramenta desenvolvida pelo LEA gerar uma requisição de um certificado digital no formato CSR PKCS#10 [11] com assinatura digital inválida e verificar se o Software de AC não valida esta requisição.

EN.I.03.04: Utilizando uma ferramenta desenvolvida pelo LEA, gerar uma requisição de um certificado digital que não utilize o formato CSR PKCS#10 [11] e verificar se o Software de AC não valida esta requisição.

REQUISITO I.04: Um Software de AC deve associar uma chave pública recebida com os dados do titular e os dados do perfil do certificado digital ambos informados pelo usuário final.

Procedimentos de ensaio para NSH 1, 2 e 3:

EN.I.04.01: Verificar se a documentação técnica do Software de AC inclui uma descrição sobre a associação de uma chave pública recebida com os dados do titular e os dados do perfil do certificado digital, ambos informados pelo usuário final.

EN.I.04.02: Utilizando uma ferramenta específica, verificar nos campos do certificado digital emitido se o Software de AC efetuou corretamente a associação da chave pública recebida com os dados do titular e com os dados do perfil do certificado digital que foram informados pelo usuário final.

REQUISITO I.05: Um Software de AC deve, antes da emissão, controlar o período de validade dos certificados digitais emitidos para AC´s ou usuários finais

solicitantes. Em termos de período de validade do certificado digital, os seguintes requisitos devem ser controlados pelo Software de AC:

- O período de validade deve estar de acordo com o tipo de certificado digital e com a PC da AC;
- o período de validade deve estar aninhado dentro do período de validade do certificado da AC emitente, obedecendo ao tipo do certificado digital.

Procedimentos de ensaio para NSH 1, 2 e 3:

EN.I.05.01: Verificar se a documentação técnica do Software de AC inclui uma descrição sobre o processo de controle do período de validade dos certificados digitais emitidos para AC´s ou usuários finais solicitantes, antes da emissão do certificado solicitado.

EN.I.05.02: Verificar se a documentação técnica do Software de AC inclui uma descrição sobre o período de validade estar de acordo com o tipo de certificado digital e com a PC da AC.

EN.I.05.03: Verificar se a documentação técnica do Software de AC inclui uma descrição sobre o período de validade estar aninhado dentro do período de validade do certificado da AC emitente, obedecendo ao tipo do certificado digital.

EN.I.05.04: Utilizando uma ferramenta desenvolvida pelo LEA, gerar requisições de certificados digitais com o período de validade inferior ou superior ao período de validade do certificado digital da AC para verificar se o Software de AC, antes da emissão do certificado, controla o período de validade não emitindo o certificado digital solicitado.

EN.I.05.05: Utilizando uma ferramenta desenvolvida pelo LEA, gerar requisições de certificados digitais e alterar a data e hora da AC para verificar se o Software de AC controla:

- O período de validade estar de acordo com o tipo de certificado digital e com a PC da AC;

- o período de validade estar aninhado dentro do período de validade do certificado da AC emitente, obedecendo ao tipo do certificado digital.

2.1.3 Requisitos de Geração e Emissão de Certificados Digitais

REQUISITO I.06: Um Software de AC deve gerar um certificado digital no formato X.509v3 de acordo com os dados de solicitação do certificado digital do usuário final, a Política de Certificação (PC) e a Declaração de Práticas de Certificação (DPC) da AC segundo as regras definidas pela ICP-Brasil.

Procedimentos de ensaio para NSH 1, 2 e 3:

EN.I.06.01: Verificar se a documentação técnica do Software de AC inclui uma descrição sobre o processo de geração de um certificado digital no formato X.509v3 de acordo com os dados de solicitação do certificado digital do usuário final, a Política de Certificação (PC) e a Declaração de Práticas de Certificação (DPC) da AC segundo as regras definidas pela ICP-Brasil.

EN.I.06.02: Utilizar uma ferramenta específica para verificar se o Software de AC gera um certificado digital no formato X.509v3 em função dos dados de solicitação do certificado digital do usuário final segundo as regras definidas pela ICP-Brasil. Para tal, validar se os dados de identificação do usuário final, sua chave pública que foi informada ao software de AC via requisição CSR PKCS#10 e o tipo do certificado digital estão em conformidade com os dados presentes no certificado digital gerado no formato X.509v3.

EN.I.06.03: Verificar se o Software de AC emite um certificado digital no formato X.509v3 de acordo com a Política de Certificação (PC) e a Declaração de Práticas de Certificação (DPC) da AC segundo as regras definidas pela ICP-Brasil. Para tal, comparar o certificado digital gerado no ensaio EN.I.06.02 com a PC da AC e verificar se o certificado digital foi gerado em conformidade com a PC da AC. Depois, comparar o certificado gerado no ensaio EN.I.06.02 com a DPC da AC e verificar se o certificado digital foi gerado em conformidade com a DPC da AC.

REQUISITO I.07: Um Software de AC deve tornar disponível um certificado digital gerado ao usuário final solicitante.

Procedimentos de ensaio para NSH 1, 2 e 3:

EN.I.07.01: Verificar se a documentação técnica do Software de AC inclui uma descrição sobre o processo de disponibilizar os certificados digitais gerados aos usuários finais solicitantes.

EN.I.07.02: Utilizar uma ferramenta desenvolvida pelo LEA para gerar requisições de certificados digitais e verificar se o Software de AC é capaz de disponibilizar os certificados digitais para um usuário final solicitante.

RECOMENDAÇÃO I.03: Um Software de AC pode entregar um componente para o usuário final com a finalidade de gerar um par de chaves criptográficas assimétricas.

Procedimentos de ensaio para NSH 1, 2 e 3:

EN.REC.I.03.01: Verificar se a documentação técnica do Software de AC inclui:

- Uma afirmação da PI informando que não suporta esta recomendação; ou
- uma descrição do componente para o usuário final com a finalidade de gerar um par de chaves criptográficas assimétricas.

EN.REC.I.03.02: Se o Software de AC possuir um componente para o usuário final com a finalidade de gerar um par de chaves criptográficas assimétricas, utilizar uma ferramenta desenvolvida pelo LEA para executar esse componente e verificar se ele gera um par de chaves criptográficas assimétricas.

REQUISITO I.08: Especificamente para certificados digitais ICP-Brasil de níveis de segurança 1 e 2, o componente do Software de AC responsável por gerar o par de chaves de forma aleatória deve utilizar métodos matemáticos seguros para esta

finalidade. Por métodos matemáticos seguros entendem-se aqueles que atendem a norma ANSI X9.31 [18] em relação ao algoritmo RSA.

Procedimentos de ensaio para NSH 1, 2 e 3:

EN.I.08.01: Verificar se a documentação técnica do Software de AC inclui uma descrição do fato do componente do Software de AC responsável por gerar o par de chaves de forma aleatória utilizar métodos matemáticos seguros para esta finalidade, especificamente para certificados digitais ICP-Brasil de níveis de segurança 1 e 2.

EN.I.08.02: Gerar pares de chaves assimétricas em relação ao algoritmo RSA utilizando o componente do Software de AC e validar se estas chaves estão utilizando os métodos descritos na norma X9.31 [18].

Procedimentos de ensaio para NSH 2 e 3:

EN.I.08.03: Verificar no código-fonte do Software de AC se este utiliza métodos matemáticos seguros para gerar o par de chaves de forma aleatória, especificamente para certificados digitais ICP-Brasil de níveis de segurança 1 e 2.

REQUISITO I.09: Um Software de AC deve permitir a emissão de certificados digitais ICP-Brasil contendo somente caracteres aceitos, conforme definido no DOC-ICP-04 [5].

Procedimentos de ensaio para NSH 1, 2 e 3:

EN.I.09.01: Verificar se a documentação técnica do Software de AC inclui uma descrição sobre o fato de permitir a emissão de certificados digitais ICP-Brasil contendo somente caracteres aceitos, conforme definido no DOC-ICP-04 [5].

EN.I.09.02: Verificar se o Software de AC emite certificados digitais ICP-Brasil contendo somente caracteres aceitos, conforme definido no DOC-ICP-04 [5]. Para

tal, utilizar a interface de solicitação de certificado digital fornecida pelo Software da AC e verificar se seus campos contêm apenas caracteres aceitos, conforme definido no DOC-ICP-04 [5].

REQUISITO I.10: Um Software de AC deve assinar certificados digitais ICP-Brasil utilizando os padrões e algoritmos definidos pela ICP-Brasil conforme DOC-ICP-01.01 [4].

Procedimentos de ensaio para NSH 1, 2 e 3:

EN.I.10.01: Verificar se a documentação técnica do Software de AC inclui uma descrição do processo de assinatura de certificados digitais ICP-Brasil utilizando os padrões e algoritmos definidos pela ICP-Brasil conforme DOC-ICP-01.01 [4].

Procedimentos de ensaio para NSH 2 e 3:

EN.I.10.02: Verificar no código-fonte do Software de AC se este assina os certificados digitais ICP-Brasil utilizando apenas os padrões e algoritmos definidos pela ICP-Brasil conforme DOC-ICP-01.01 [4].

REQUISITO I.11: Um Software de AC deve permitir a emissão de certificados digitais ICP-Brasil para AC Raiz [3], AC´s intermediárias ou usuários finais.

Procedimentos de ensaio para NSH 1, 2 e 3:

EN.I.11.01: Verificar se a documentação técnica do Software de AC inclui uma descrição do processo de emissão de certificados digitais ICP-Brasil para AC Raiz [3], AC´s intermediárias ou usuários finais.

EN.I.11.02: Verificar se o Software de AC permite a emissão de certificados digitais ICP-Brasil para AC Raiz [3], AC´s intermediárias ou usuários finais. Para tal, acessar o Software de AC e verificar se este disponibiliza, entre as suas funcionalidades, a

geração de certificados digitais ICP-Brasil para AC Raiz [3], AC´s intermediárias ou usuários finais.

REQUISITO I.12: Um Software de AC deve possuir meios necessários para manter a relação unívoca entre um par de chaves criptográficas assimétricas e um usuário final. Este requisito tem o objetivo de evitar com que usuários finais maliciosos solicitem certificados digitais diferentes a uma AC utilizando o mesmo par de chaves assimétricas, fato este que se ocorrer pode possibilitar a geração de assinaturas digitais idênticas (homônimas) que não evitam a irretratabilidade de conteúdo e de geração da assinatura digital.

Procedimentos de ensaio para NSH 1, 2 e 3:

EN.I.12.01: Verificar se a documentação técnica do Software de AC inclui uma descrição dos meios necessários para manter a relação unívoca entre um par de chaves criptográficas assimétricas e um usuário final.

EN.I.12.02: Utilizar uma ferramenta desenvolvida pelo LEA para gerar duas requisições de certificados digitais idênticas e enviá-las para o Software da AC e verificar que a AC, para manter a relação unívoca entre um par de chaves criptográficas e um usuário final, não deve emitir o segundo certificado digital solicitado.

2.1.4 Requisitos de Renovação de Certificados Digitais

REQUISITO I.13: Um Software de AC deve oferecer uma interface e funcionalidades necessárias que permitam aos usuários finais renovarem seus certificados digitais. Conforme definido no glossário ICP-Brasil [8], renovação de certificado digital ICP-Brasil significa o processo para obter um certificado novo antes que o certificado existente tenha expirado. Na ICP-Brasil, é obrigatória a geração de novas chaves criptográficas distintas para cada certificado emitido.

Procedimentos de ensaio para NSH 1, 2 e 3:

EN.I.13.01: Verificar se a documentação técnica do Software de AC inclui uma descrição de uma interface e de funcionalidades necessárias que permitam aos usuários finais renovarem seus certificados digitais.

EN.I.13.02: Utilizar a interface de renovação de certificado digital fornecida pelo Software da AC e com um certificado digital ativo e operacional de um usuário final com período de validade inferior a 30 dias, efetuar a renovação deste certificado digital. Depois, verificar que os dados contidos do novo certificado digital emitido são os mesmo do certificado digital anterior, alterando somente a chave pública.

EN.I.13.03: Utilizar a interface de renovação de certificado digital fornecida pelo Software da AC e com um certificado digital ativo e operacional de um usuário final que foi gerado no EN.I.13.02, tentar efetuar a renovação deste certificado digital e verificar que o Software de AC não deve permitir a renovação de um certificado que já foi renovado anteriormente.

EN.I.13.04: Utilizar a interface de renovação de certificado digital fornecida pelo Software da AC e com um certificado digital ativo e operacional de um usuário final com período de validade superior a 30 dias, tentar efetuar a renovação deste certificado digital e verificar que o Software da AC não deverá emitir a renovação deste certificado.

EN.I.13.05: Utilizar a interface de renovação de certificado digital fornecida pelo Software da AC e com um certificado digital revogado de um usuário final, tentar efetuar a renovação deste certificado digital e verificar que o Software da AC não deverá emitir a renovação deste certificado.

REQUISITO I.14: Ao decorrer de um processo de renovação de certificado digital ICP-Brasil, um Software de AC deve verificar se o usuário final gerou uma chave pública diferente das chaves públicas presentes nos certificados digitais anteriores. Este requisito tem por finalidade evitar com que o usuário final consiga renovar o seu certificado digital utilizando a mesma chave pública de algum certificado digital anteriormente emitido.

Procedimentos de ensaio para NSH 1, 2 e 3:

EN.I.14.01: Verificar se a documentação técnica do Software de AC contém informações, para o processo de renovação de certificados digitais ICP-Brasil, sobre a verificação após usuário final gerar uma chave pública diferente das chaves públicas presentes nos certificados digitais anteriores.

EN.I.14.02: Utilizar a interface de renovação de certificado digital fornecida pelo Software da AC e com um certificado digital ativo e operacional de um usuário final, tentar efetuar a renovação deste certificado digital utilizando a mesma requisição do certificado digital a ser renovado e verificar que Software da AC não deverá emitir a renovação deste certificado.

REQUISITO I.15: Ao decorrer de um processo de renovação de certificado digital ICP-Brasil, um Software de AC deve também consultar e verificar se a nova chave pública utilizada pelo usuário final na renovação é diferente das chaves públicas certificadas por todas as outras AC´s de mesmo nível credenciadas na ICP-Brasil. Este requisito tem por finalidade evitar com que o usuário final consiga renovar o seu certificado digital utilizando a mesma chave pública de algum certificado digital anteriormente emitido por uma AC diferente daquela escolhida para a solicitação atual.

Procedimentos de ensaio para NSH 1, 2 e 3:

EN.I.15.01: Verificar se a documentação técnica do Software de AC contém informações, para o processo de renovação de certificados digitais ICP-Brasil, sobre a consulta e a verificação da nova chave pública utilizada pelo usuário final na renovação ser diferente das chaves públicas certificadas por todas as outras AC´s de mesmo nível credenciadas na ICP-Brasil.

EN.I.15.02: Instalar pelo menos duas instâncias do Software de AC, considerando AC's distintas, e gerar uma requisição para renovação de um certificado digital para

pelo menos uma dessas AC's. Verificar que o Software de AC não deve permitir a renovação do certificado digital se na outra AC contiver a chave pública igual à chave pública da requisição da renovação.

REQUISITO I.16: O software de AC deve controlar que o pedido de renovação seja feito dentro do período de validade do certificado digital.

Procedimentos de ensaio para NSH 1, 2 e 3:

EN.I.16.01: Verificar se a documentação técnica do Software de AC inclui uma descrição do processo de controlar que o pedido de renovação seja feito dentro do período de validade do certificado digital.

EN.I.16.02: Utilizar a interface de renovação de certificado digital fornecida pelo Software da AC e com um certificado digital expirado de um usuário final, tentar efetuar a renovação deste certificado digital e verificar que Software da AC não deverá emitir a renovação deste certificado.

2.1.5 Requisitos de Revogação de Certificados Digitais

Dentro do período de validade, um usuário final pode solicitar a revogação de um certificado digital por vários motivos, como comprometimento da própria chave privada, certificado digital gerado com dados errados do titular etc.
A AC que emitiu o certificado digital de um usuário final pode também revogar o seu certificado por motivos de renovação do par de chaves da AC, comprometimento do par de chaves da AC etc.

REQUISITO I.17: Um Software de AC deve fornecer ao usuário final uma interface de revogação de certificados digitais.

Procedimentos de ensaio para NSH 1, 2 e 3:

EN.I.17.01: Verificar se a documentação técnica do Software de AC descreve sobre uma interface de revogação de certificados digitais.

EN.I.17.02: Realizar uma revogação de um certificado digital utilizando a interface descrita na documentação e verificar se o certificado foi revogado corretamente. Depois, verificar se o certificado consta na lista mais recente de certificados revogados.

REQUISITO I.18: Um Software de AC deve receber requisições de revogação de certificados digitais.

Procedimentos de ensaio para NSH 1, 2 e 3:

EN.I.18.01: Verificar se a documentação técnica do Software de AC descreve sobre a capacidade do software de receber requisições de revogação de certificados digitais.

EN.I.18.02: Realizar uma requisição de revogação de um certificado digital utilizando as interfaces de revogação de certificados digitais do software de AC e verificar se esse processo é gerado sem erros.

REQUISITO I.19: Antes de permitir a revogação, um Software de AC deve tornar disponível ao usuário final um mecanismo de autenticação para a revogação de seu certificado digital. Portanto, o Software de AC deve ser capaz de aceitar requisições de revogação somente após o titular do certificado digital ter sido previamente autenticado.

Procedimentos de ensaio para NSH 1, 2 e 3:

EN.I.19.01: Verificar se a documentação técnica do Software de AC descreve sobre um mecanismo de autenticação para a revogação do certificado digital do usuário final, antes de permitir a revogação.

EN.I.19.02: Utilizar a interface de revogação de certificados digitais do software de AC para tentar revogar um certificado digital sem fazer uma autenticação prévia no Software de AC e verificar que este não permite a revogação.

EN.I.19.03: Utilizar a interface de revogação de certificados digitais do software de AC para tentar revogar um certificado digital apresentando uma falsa autenticação no Software de AC e verificar que este não permite a revogação.

RECOMENDAÇÃO I.04: Um Software de AC pode ter mecanismos de notificação para os titulares de certificados digitais, por exemplo, por meio do envio de *e-mails*, quando ocorrer suspeita de comprometimento da chave privada da AC, emissão de novo par de chaves e correspondente certificado, ou então o encerramento de suas atividades.

Procedimentos de ensaio para NSH 1, 2 e 3:

EN.REC.I.04.01: Verificar se a documentação técnica do Software de AC inclui:

- Uma afirmação da PI informando que não suporta esta recomendação; ou
- Verificar se a documentação técnica descreve os mecanismos de notificação que são utilizados pelo software de AC para alertar os titulares de certificados digitais, quando ocorrer suspeita de comprometimento da chave privada da AC, emissão de novo par de chaves e correspondente certificado, ou então o encerramento de suas atividades.

EN.REC.I.04.02: Caso o Software de AC suporte esta recomendação, tentar realizar uma ou mais das seguintes ações:

- comprometimento da chave privada da AC onde se deve:
    - emitir um novo par de chaves da AC e seu correspondente certificado;
    - emitir todos os certificados digitais dos titulares;
- encerramento das atividades da AC.

Depois, verificar se o titular do certificado foi notificado pela ação ou ações tomadas.

RECOMENDAÇÃO I.05: Recomenda-se que um Software de AC não retire da LCR um certificado digital que foi revogado e posteriormente expirado.

Procedimentos de ensaio para NSH 1, 2 e 3:

EN.REC.I.05.01: Verificar se a documentação técnica do Software de AC inclui:
●Uma afirmação da PI informando que não suporta esta recomendação;ou
●Verificar se a documentação técnica descreve como o software de AC controla os certificados digitais expirados na LCR.

EN.REC.I.05.02: Se o Software de AC suporta esta recomendação, inicialmente emitir um certificado digital. Depois, alterar a data e hora da AC para que o período de validade do certificado digital emitido seja, por exemplo, de um dia de duração. Então, realizar a revogação desse certificado e esperar o tempo necessário para expirar o certificado emitido. Á partir da LCR emitida, logo após o tempo de expiração do certificado, verificar se o certificado revogado não deixou de existir na LCR mais recente.

REQUISITO I.20: Um Software de AC deve gerar LCR´s de acordo com o DOC-ICP-04 [5].

Procedimentos de ensaio para NSH 1, 2 e 3:

EN.I.20.01: Verificar se a documentação técnica do Software de AC descreve que a geração de LCR´s está de acordo com o DOC-ICP-04 [5].

EN.I.20.02: Utilizar uma ferramenta desenvolvida pelo LEA para verificar se o perfil de uma LCR gerada pelo Software de AC está de acordo com o DOC-ICP-04 [5].

REQUISITO I.21: Um Software de AC deve publicar automaticamente a última LCR em repositórios internos e especificamente definidos pela AC para livre consulta. Antes da publicação de uma LCR, o Software de AC deve verificar se as seguintes condições foram satisfeitas:

●O certificado digital da AC que assina a LCR deve ser válido e possuir o campo *Key Usage* com valor *CRLSign* ativo;
●o repositório interno de publicação da AC deve ter o mesmo endereço do campo *CRL Distribution Point* informado nos respectivos certificados digitais emitidos para usuários finais.

Procedimentos de ensaio para NSH 1, 2 e 3:

EN.I.21.01: Verificar se a documentação técnica do Software de AC descreve sobre o processo de publicação automática da última LCR em repositórios internos e especificamente definidos pela AC para livre consulta.

EN.I.21.02: Verificar se a documentação técnica do Software de AC descreve sobre o processo de verificação das condições citadas no REQUISITO I.21.

EN.I.21.03: Utilizar a interface de revogação de certificados digitais do Software de AC para revogar um certificado digital e verificar se o Software de AC publica automaticamente a última LCR em repositórios internos e nos repositórios especificamente definidos pela AC para livre consulta.

EN.I.21.04: Utilizar uma ferramenta desenvolvida pelo LEA para verificar se:
●O certificado digital da AC que assina a LCR é válido e possui o campo *Key Usage* com valor *CRLSign* ativo;
●o repositório interno de publicação da AC tem o mesmo endereço do campo *CRL Distribution Point* informado em um certificado digital emitido pelo Software de AC para usuários finais.

REQUISITO I.22: Conforme o DOC-ICP-05 [7], um Software de AC deve fornecer interfaces de revogação de certificados digitais customizadas para cada entidade:

- Usuário final;
- AC.

Procedimentos de ensaio para NSH 1, 2 e 3:

EN.I.22.01: Verificar se a documentação técnica do Software de AC descreve as interfaces de revogação de certificados digitais customizadas para cada entidade que a acesse.

EN.I.22.02: Verificar se o software de AC possui interfaces de revogação de certificados digitais customizadas para as seguintes entidades:

- Usuário final; e
- AC.

EN.I.22.03: Realizar a revogação de um certificado digital utilizando a interface de revogação de certificados digitais para o usuário final.

EN.I.22.04: Realizar a revogação de um certificado digital utilizando a interface de revogação de certificados digitais para a AC.

REQUISITO I.23: Um Software de AC deve registrar as solicitações de revogação de certificados digitais.

Procedimentos de ensaio para NSH 1, 2 e 3:

EN.I.23.01: Verificar se a documentação técnica do Software de AC descreve sobre o processo de registro das solicitações de revogação de certificados digitais.

EN.I.23.02: Utilizar a interface de revogação de certificados digitais do Software de AC para revogar um certificado digital e verificar se o Software de AC registra (em um banco de dados, por exemplo) as solicitações de revogação de certificados digitais.

2.1.5.1 Listas de Certificados Revogados

DEFINIÇÃO: Conforme definido no glossário ICP-Brasil [8], uma lista de certificados revogados é uma lista assinada digitalmente por uma Autoridade Certificadora, publicada periodicamente, contendo certificados que foram revogados antes de

suas respectivas datas de expiração. A lista, geralmente, indica o nome de quem a emite, a data de emissão e a data da próxima emissão programada, além dos números de série dos certificados revogados e a data da revogação.

REQUISITO I.24: Um Software de AC deve permitir a configuração do caminho de publicação de LCR´s.

Procedimentos de ensaio para NSH 1, 2 e 3:

EN.I.24.01: Verificar se a documentação técnica do Software de AC descreve sobre a configuração do caminho de publicação de LCR´s.

EN.I.24.02: Utilizar a interface de revogação de certificados digitais do Software de AC e verificar se este possui a opção de configurar o caminho de publicação de LCR ´s.

REQUISITO I.25: Um Software de AC deve garantir a gravação/publicação da LCR no repositório configurado.

Procedimentos de ensaio para NSH 1, 2 e 3:

EN.I.25.01: Verificar se a documentação técnica do Software de AC descreve sobre a gravação/publicação da LCR no repositório configurado.

EN.I.25.02: Utilizar a interface de revogação de certificados digitais do Software de AC para configurar o caminho de publicação de LCR´s. Depois, verificar se a LCR é gravada/publicada no caminho configurado.

REQUISITO I.26: Um Software de AC deve publicar uma LCR segundo os padrões e normas definidas pelo ICP-Brasil no DOC-ICP-04 [5] em função do tipo do certificado digital.

Procedimentos de ensaio para NSH 1, 2 e 3:

EN.I.26.01: Verificar se a documentação técnica do Software de AC descreve que a publicação de uma LCR segue os padrões e normas definidas pelo ICP-Brasil no DOC-ICP-04 [5] em função do tipo do certificado digital.

EN.I.26.02: Revogar um certificado digital e verificar se a LCR publicada pelo Software de AC segue os padrões e normas definidas pelo ICP-Brasil no DOC-ICP-04 [5] em função do tipo do certificado digital.

RECOMENDAÇÃO I.06: Um Software de AC pode configurar pontos distintos de distribuição da LCR para fins de contingência.

Procedimentos de ensaio para NSH 1, 2 e 3:

EN.REC.I.06.01: Verificar se a documentação técnica do Software de AC inclui:
- Uma afirmação da PI informando que não suporta esta recomendação; ou
- uma descrição sobre a configuração dos pontos distintos de distribuição da LCR para fins de contingência.

EN.REC.I.06.02: Se o Software de AC suporta esta recomendação, verificar que o Software de AC consegue configurar pontos distintos de distribuição da LCR para fins de contingência.

REQUISITO I.27: Um Software de AC deve assinar as LCR´s com a mesma chave privada usada para assinar os certificados digitais.

Procedimentos de ensaio para NSH 1, 2 e 3:

EN.I.27.01: Verificar se a documentação técnica do Software de AC descreve que o processo de assinatura das LCR´s é feito com a mesma chave privada usada para assinar os certificados digitais.

EN.I.27.02: Utilizar uma ferramenta desenvolvida pelo LEA para verificar se o software de AC assina as LCR´s com a mesma chave privada usada para assinar os certificados digitais.

REQUISITO I.28: Um Software de AC deve emitir LCR´s na data e hora estabelecidos pelo campo *nextUpdate* da LCR vigente que define a próxima data e hora de publicação.

Procedimentos de ensaio para NSH 1, 2 e 3:

EN.I.28.01: Verificar se a documentação técnica do Software de AC descreve que a emissão de LCR´s é feita na data e hora estabelecidos pelo campo *nextUpdate* da LCR vigente que define a próxima data e hora de publicação.

EN.I.28.02: Revogar um certificado digital para verificar se o software de AC emite LCR´s na data e hora estabelecidos pelo campo *nextUpdate* da LCR vigente que define a próxima data e hora de publicação em função do tipo do certificado digital.

REQUISITO I.29: Um Software de AC deve permitir a publicação automática ou manual de LCR´s. Por publicação automática entende-se uma publicação de LCR realizada diretamente pelo Software de AC sem a necessidade de intervenção do operador. Por publicação manual entende-se uma publicação de LCR realizada com a intervenção do operador.

Procedimentos de ensaio para NSH 1, 2 e 3:

EN.I.29.01: Verificar se a documentação técnica do Software de AC descreve que este permite a publicação automática ou manual de LCR´s.

EN.I.29.02: Verificar se a documentação técnica do Software de AC descreve o processo de publicação automática ou manual de LCR´s ou ainda de ambos.

EN.I.29.03: Revogar um certificado digital para verificar se o software de AC gera a publicação automática e/ou manual de LCR´s e verificar se a publicação é feita corretamente.

2.1.6 Requisitos para a Utilização de OCSP

Os requisitos para a utilização do serviço de OCSP são requisitos condicionais que dependem de uma ICP ter tal serviço disponível para uso pelos usuários finais. Deve-se mencionar que conforme recomendação I.02, o serviço de OCSP é opcional e pode ser oferecido por uma ICP.
Dentro de uma ICP, o serviço de OCSP pode ser configurado como um componente separado do Software de AC ou como um componente integrante do Software de AC.

REQUISITO I.30: Caso uma ICP ofereça o serviço de OCSP, um Software de AC deve ter funcionalidade para publicar no repositório OCSP as informações sobre um certificado digital revogado.

Procedimentos de ensaio para NSH 1, 2 e 3:

EN.I.30.01: Verificar se a documentação técnica do Software de AC inclui:
- Uma afirmação da PI informando que não suporta este serviço; ou
- uma descrição sobre a funcionalidade para publicar no repositório OCSP as informações sobre um certificado digital revogado.

EN.I.30.02: Se o Software de AC oferecer a funcionalidade para publicar no repositório OCSP as informações sobre um certificado digital revogado, revogar um certificado digital e por meio do serviço de OCSP, utilizando uma ferramenta desenvolvida pelo LEA, verificar se o certificado revogado encontra-se publicado no repositório OCSP.

REQUISITO I.31: Caso um Software de AC tenha um componente de software para prover o serviço de OCSP, o Software de AC deve controlar que todas as respostas OCSP sejam assinadas digitalmente utilizando um certificado digital válido com

propósitos de uso também válidos. Além disso, o Software de AC deve assegurar que as respostas OCSP sejam geradas conforme as regras definidas na RFC 2560 [14].

Procedimentos de ensaio para NSH 1, 2 e 3:

EN.I.31.01: Verificar se a documentação técnica do Software de AC inclui:
●Uma afirmação da PI informando que não possui um componente de software para este serviço; ou
●uma descrição do processo de controle para que todas as respostas OCSP sejam assinadas digitalmente utilizando um certificado digital válido com propósitos de uso também válidos.

EN.I.31.02: Se o Software de AC tiver um componente de software para prover o serviço de OCSP, verificar na documentação técnica do Software de AC se as regras definidas na RFC 2560 [14] foram seguidas para a geração das respostas de OCSP.

EN.I.31.03: Se o Software de AC oferecer a funcionalidade para publicar no repositório OCSP as informações sobre um certificado digital revogado e utilizando uma ferramenta desenvolvida pelo LEA, verificar se:
●Todas as respostas OCSP são assinadas digitalmente utilizando um certificado digital válido com propósitos de uso também válidos;
●as respostas OCSP são geradas conforme as regras definidas na RFC 2560 [14].

Procedimentos de ensaio para NSH 2 e 3:

EN.I.31.04: Verificar no código-fonte do Software de AC se o componente de software para prover o serviço de OCSP está aderente as regras definidas na RFC 2560 [14].

2.1.7 Requisitos de Configuração do Software de AC

A seção de requisitos de configuração trata a administração e configuração do Software de AC.

REQUISITO I.32: Uma interface de administração do Software de AC deve permitir configurar o Software de AC e as operações de configuração devem ser realizadas por um administrador. Portanto, a interface de administração do Software de AC deve, no mínimo, permitir com que as seguintes operações sejam realizadas:

- Configuração do componente que emite certificados;
- configuração da hierarquia de certificação digital da AC;
- configuração de controle de acesso e autenticação;
- configuração de geração e monitoração de registros (logs);
- configuração de repositórios;
- configuração de publicações.

Procedimentos de ensaio para NSH 1, 2 e 3:

EN.I.32.01: Verificar se a documentação técnica do Software de AC descreve sobre a interface de administração do Software de AC.

EN.I.32.02: Verificar se a documentação técnica do Software de AC descreve que a configuração do Software de AC é feita pela interface de administração do Software de AC e que as operações de configuração são realizadas por um administrador.

EN.I.32.03: Verificar se a documentação técnica do Software de AC descreve que a interface de administração do Software de AC permite, no mínimo, com que as seguintes operações sejam realizadas:

- Configuração do componente que emite certificados;
- configuração da hierarquia de certificação digital da AC;
- configuração de controle de acesso e autenticação;
- configuração de geração e monitoração de registros (logs);
- configuração de repositórios;
- configuração de publicações.

EN.I.32.04: Utilizar a interface de administração do Software de AC para verificar se todas as opções de configuração descritas na documentação estão disponíveis e operacionais.

EN.I.32.05: Utilizar a interface de administração do Software de AC para verificar se as funcionalidades decorrentes das configurações feitas estão funcionando corretamente.

REQUISITO I.33: Um Software de AC deve gerar e manter os seguintes tipos de certificados:

- Certificados digitais com propósitos específicos para AC´s intermediárias; ou
- certificados digitais com propósitos específicos para utilização por usuários finais.

Procedimentos de ensaio para NSH 1, 2 e 3:

EN.I.33.01: Verificar se a documentação técnica do Software de AC descreve sobre o processo de gerar e manter os seguintes tipos de certificados:

- Certificados digitais com propósitos específicos para AC´s intermediárias; ou
- certificados digitais com propósitos específicos para utilização por usuários finais.

EN.I.33.02: Utilizar a interface do Software de AC para gerar certificados digitais com propósitos específicos para AC´s intermediárias e/ou certificados digitais com propósitos específicos para utilização por usuários finais. Depois verificar se o Software de AC mantém (em um banco de dados ou repositório específico) esses certificados digitais gerados.

REQUISITO I.34: Um Software de AC deve permitir a criação, configuração e manutenção de modelos padronizados (*templates*) para a geração de certificados digitais em função do tipo de certificado definido pela ICP-Brasil.

Procedimentos de ensaio para NSH 1, 2 e 3:

EN.I.34.01: Verificar se a documentação técnica do Software de AC descreve sobre o processo de criação, configuração e manutenção de modelos padronizados (*templates*) para a geração de certificados digitais em função do tipo de certificado definido pela ICP-Brasil.

EN.I.34.02: Utilizar a interface do Software de AC para configurar e gerar um modelo padronizado (*template*) para a geração de certificados digitais em função de um tipo de certificado definido pela ICP-Brasil, por exemplo A3. Depois, utilizando uma ferramenta desenvolvida pelo LEA, verificar se o certificado gerado corresponde aos dados configurados no *template.*

REQUISITO I.35: Um certificado digital gerado e utilizado pelo Software de AC deve seguir as normas e os formatos definidos pela ICP-Brasil.

Procedimentos de ensaio para NSH 1, 2 e 3:

EN.I.35.01: Verificar se a documentação técnica do Software de AC contém informações sobre o fato dos certificados digitais gerados e utilizados pelo Software de AC seguirem as normas e os formatos definidos pela ICP-Brasil.

EN.I.35.02: Utilizar a interface do Software de AC para gerar um certificado digital e , utilizando uma ferramenta específica, verificar se este certificado digital segue as normas e os formatos definidos pela ICP-Brasil.

REQUISITO I.36: Baseando-se no tipo de certificado digital ICP-Brasil (A1, A2, A3, A4, S1, S2, S3, S4, T3 ou T4) e na PC definida pela AC, um Software de AC deve permitir sua configuração para atender o subconjunto de extensões X509v3 e os propósitos de uso que devem ser utilizados na emissão de um certificado digital.

Procedimentos de ensaio para NSH 1, 2 e 3:

EN.I.36.01: Verificar se a documentação técnica do Software de AC descreve sobre a configuração do Software de AC para atender o subconjunto de extensões X509v3 e os propósitos de uso que devem ser utilizados na emissão de um certificado digital, baseando-se no tipo de certificado digital ICP-Brasil e na PC definida pela AC.

EN.I.36.02: Utilizar a interface do Software de AC para configurar o subconjunto de extensões X509v3 e os propósitos de uso, baseando-se no tipo de certificado digital ICP-Brasil (A1, A2, A3, A4, S1, S2, S3, S4, T3 ou T4) e na PC definida pela AC, que devem ser utilizados na emissão de um certificado digital. Depois, verificar se no certificado digital emitido estão contidos os dados que refletem a configuração realizada.

REQUISITO I.37: Um Software de AC deve configurar a emissão de certificados digitais ICP-Brasil conforme definido pelo DOC-ICP-04 [5].

Procedimentos de ensaio para NSH 1, 2 e 3:

EN.I.37.01: Verificar se a documentação técnica do Software de AC descreve sobre a configuração para a emissão de certificados digitais ICP-Brasil conforme definido pelo DOC-ICP-04 [5].

EN.I.37.02: Emitir um certificado digital pelo Software de AC e, utilizando uma ferramenta desenvolvida pelo LEA, verificar neste certificado digital emitido se as opções de configuração para emissão de certificados digitais ICP-Brasil atendem o DOC-ICP-04 [5].

REQUISITO I.38: Um Software de AC deve permitir a configuração de políticas parametrizáveis para certificados e para LCR´s de acordo com o DOC-ICP-04 [5].

Procedimentos de ensaio para NSH 1, 2 e 3:

EN.I.38.01: Verificar se a documentação técnica do Software de AC descreve sobre a configuração de políticas parametrizáveis para certificados e para LCR´s e que estejam de acordo com o DOC-ICP-04 [5].

EN.I.38.02: Emitir um certificado digital utilizando a interface do Software de AC e verificar se as opções de configuração de políticas parametrizáveis para certificados atendem o DOC-ICP-04 [5].

EN.I.38.03: Revogar um certificado digital utilizando a interface do Software de AC e verificar se as opções de configuração de políticas parametrizáveis para LCR´s atendem o DOC-ICP-04 [5].

2.1.8 Requisitos de Interoperabilidade

REQUISITO I.39: Um Software de AC deve aceitar requisições e emitir certificados digitais conforme os seguintes tipos de codificações:

- Binário:
  - BER [9];
  - DER [9];
- texto:
  - PEM [12];
  - Base64 [17].

Procedimentos de ensaio para NSH 1, 2 e 3:

EN.I.39.01: Verificar se a documentação técnica do Software de AC descreve sobre as requisições e emissões de certificados digitais para cada um dos tipos de codificações do REQUISITO I.39.

EN.I.39.02: Utilizar uma ferramenta específica para gerar requisições de certificados digitais no formato CSR PKCS#10 [11] para cada um dos tipos de codificações do REQUISITO I.39 e verificar se o Software de AC emite os certificados digitais solicitados também para cada um dos tipos de codificações.

Procedimentos de ensaio para NSH 2 e 3:

EN.I.39.03: Verificar no código-fonte do Software de AC se as requisições e emissões de certificados digitais atendem à cada um dos tipos de codificações do REQUISITO I.39.

RECOMENDAÇÃO I.07: Um Software de AC pode emitir certificados digitais ICP-Brasil que estejam contidos em um conteúdo CMS [15] ou PKCS#7 [10].

Procedimentos de ensaio para NSH 1, 2 e 3:

EN.REC.I.07.01: Verificar se a documentação técnica do Software de AC inclui:
- Uma afirmação da PI informando que não suporta esta recomendação; ou
- uma descrição sobre a emissão de certificados digitais ICP-Brasil que estejam contidos em um conteúdo CMS [15] ou PKCS#7 [10].

EN.REC.I.07.02: Caso o Software da AC suporte esta recomendação, emitir um certificado digital e, utilizando uma ferramenta desenvolvida pelo LEA, verificar se este certificado digital emitido está contido em um conteúdo CMS [15] ou PKCS#7 [10].

RECOMENDAÇÃO I.08: Um Software de AC pode permitir a entrega de um certificado digital ICP-Brasil para um usuário final que esteja contido em um conteúdo CMS [15] ou PKCS#7 [10] incluindo a respectiva cadeia de certificação.

Procedimentos de ensaio para NSH 1, 2 e 3:

EN.REC.I.08.01: Verificar se a documentação técnica do Software de AC inclui:
- Uma afirmação da PI informando que não suporta esta recomendação; ou
- uma descrição sobre a entrega de um certificado digital ICP-Brasil para um usuário final que esteja contido em um conteúdo CMS [15] ou PKCS#7 [10] incluindo a respectiva cadeia de certificação.

EN.REC.I.08.02: Caso o Software da AC suporte esta recomendação, emitir um certificado digital e, utilizando uma ferramenta desenvolvida pelo LEA, verificar se este certificado digital emitido está contido em um conteúdo CMS [15] ou PKCS#7 [10] incluindo a respectiva cadeia de certificação.

2.1.9 Requisitos de Gerenciamento

Nesta seção serão abordados os requisitos sobre o gerenciamento de uma AC.

REQUISITO I.40: Um Software de AC deve dispor ao operador/administrador uma interface para gerenciar certificados. Esta interface deve atender, no mínimo, as seguintes funcionalidades:

- Requisições de certificados:
  - processar requisições:
    - aceitar;
    - rejeitar;
    - cancelar;
  - listar requisições de certificados;
- listar certificados:
  - emitidos;
  - expirados;
  - revogados;
- renovar e revogar certificados;
- gerenciar a lista de certificados revogados;
- publicação de certificados emitidos e LCR;
- recuperação de dados.

Procedimentos de ensaio para NSH 1, 2 e 3:

EN.I.40.01: Verificar se a documentação técnica do Software de AC descreve sobre a interface para gerenciar certificados disponibilizada ao operador e ao administrador.

EN.I.40.02: Verificar se a documentação técnica do Software de AC descreve, no mínimo, sobre as funcionalidades descritas no REQUISITO.I.40.

EN.I.40.03: Verificar no Software de AC se este possui uma interface para gerenciar os certificados digitais. Depois, verificar se essa interface disponibiliza, no mínimo, as funcionalidades descritas no REQUISITO.I.40.

REQUISITO I.41: Uma interface entre o Software de AC e o usuário final deve permitir, no mínimo, a realização das seguintes funcionalidades:

- Solicitar um certificado digital;
- obter o certificado digital solicitado;
- consultar certificados digitais emitidos;
- requisitar a revogação de um certificado digital;
- obter informações de revogação do certificado digital (LCR ou OCSP);
- obter o caminho de certificação.

Procedimentos de ensaio para NSH 1, 2 e 3:

EN.I.41.01: Verificar se a documentação técnica do Software de AC descreve sobre a interface entre o Software de AC e o usuário final.

EN.I.41.02: Verificar se a documentação técnica do Software de AC descreve, no mínimo, sobre as funcionalidades descritas no REQUISITO.I.41.

EN.I.41.03: Verificar no Software de AC se este possui uma interface entre o Software de AC e o usuário final. Depois, verificar se essa interface disponibiliza, no mínimo, as funcionalidades descritas no REQUISITO.I.41.

2.1.10 Requisitos de Segurança

Esta subseção descreve os requisitos relacionados com a segurança do Software de AC, tais como:

- Papel de acesso;
- auditoria;

- arquivamento de chaves privadas;
- interação com o *hardware* seguro.

2.1.10.1 Requisitos de Papel de Acesso de um Software de AC

REQUISITO I.42: Um Software de AC deve permitir ao operador da AC se autenticar, no mínimo, por meio de *login* e senha.

Procedimentos de ensaio para NSH 1, 2 e 3:

EN.I.42.01: Verificar se a documentação técnica do Software de AC descreve sobre o processo de autenticação do operador de AC.

EN.I.42.02: Verificar se a documentação técnica do Software de AC descreve que o processo de autenticação do operador de AC é feito, no mínimo, por meio de *login* e senha.

EN.I.42.03: Acessar o Software da AC com autenticação por meio de *login* e senha de um operador da AC e verificar se o papel do acesso está compatível com o de um operador de AC.

Procedimentos de ensaio para NSH 2 e 3:

EN.I.42.04: Verificar no código-fonte do Software de AC se as autenticações feitas por meio de *login* e senha de um operador da AC não são realizadas internamente no código.

REQUISITO I.43: Um Software de AC deve ter funcionalidade para a criação, alteração, suspensão temporária e exclusão de um perfil de operador da AC. Na criação ou na alteração do perfil de operador, o Software de AC deve vincular os dados do *login* ou do certificado digital que o operador da AC deve utilizar para acessar o software.

Procedimentos de ensaio para NSH 1, 2 e 3:

EN.I.43.01: Verificar se a documentação técnica do Software de AC descreve sobre a funcionalidade para a criação, alteração, suspensão temporária e exclusão de um perfil de operador da AC.

EN.I.43.02: Verificar se a documentação técnica do Software de AC descreve que na criação ou na alteração do perfil de operador, o Software de AC vincula os dados do *login* ou do certificado digital que o operador da AC utiliza para acessar o software.

EN.I.43.03: Acessar o Software da AC para verificar se este possui as funcionalidades de criação, alteração, suspensão temporária e exclusão de um perfil de operador da AC.

EN.I.43.04: Utilizar o Software da AC para criar ou alterar o perfil de um operador e verificar se o Software da AC vincula os dados do *login* ou do certificado digital, que o operador da AC utiliza para acessar o software, em sua base de dados.

Procedimentos de ensaio para NSH 2 e 3:

EN.I.43.05: Verificar no código-fonte do Software de AC se a funcionalidade para a alteração, suspensão temporária e exclusão de um perfil de operador da AC não é realizada com este operador da AC autenticado.

REQUISITO I.44: Um Software de AC deve ter funcionalidade para a criação, alteração, suspensão temporária e exclusão de um perfil de operador da AR. Na criação ou na alteração do perfil de operador, o Software de AC deve vincular o certificado digital A3 que o operador da AR deve utilizar para acessar o software.

Procedimentos de ensaio para NSH 1, 2 e 3:

EN.I.44.01: Verificar se a documentação técnica do Software de AC descreve sobre a funcionalidade para a criação, alteração, suspensão temporária e exclusão de um perfil de operador da AR.

EN.I.44.02: Verificar se a documentação técnica do Software de AC descreve que na criação ou na alteração do perfil de operador, o Software de AC vincula o certificado digital A3 que o operador da AR utiliza para acessar o software.

EN.I.44.03: Acessar o Software da AC para verificar se este possui as funcionalidades de criação, alteração, suspensão temporária e exclusão de um perfil de operador da AR.

EN.I.44.04: Utilizar o Software da AC para criar ou alterar o perfil de um operador de AR e verificar se o Software da AC vincula o certificado digital A3, que o operador da AR utiliza para acessar o software, em sua base de dados.

2.1.10.2 Requisitos de Auditoria de Software de AC

REQUISITO I.45: Um Software de AC deve gerar, no mínimo, os seguintes registros de auditoria para:

- Controle de acesso:
  - registros relacionados ao controle de acesso;
- autenticação:
  - registros relacionados às atividades de autenticação;
- autoridade certificadora:
  - registros relacionados às atividades desempenhadas pelo subsistema gerente de certificados;
- banco de dados:
  - registros relacionados às atividades desempenhadas com o banco de dados;
- HTTP:
  - registros relacionados às atividades desempenhadas com o servidor web que interage com os usuários finais;
- repositório de publicação:

- registros relacionados às atividades dos repositório de publicação (certificados emitidos e LCR´s).

Procedimentos de ensaio para NSH 1, 2 e 3:

EN.I.45.01: Verificar se a documentação técnica do Software de AC descreve sobre os seus registros de auditoria.

EN.I.45.02: Verificar se a documentação técnica do Software de AC descreve que, no mínimo, o Software de AC gera os registros descritos no REQUISITO I.45.

EN.I.45.03: Utilizar o Software de AC e verificar se este gera, no mínimo, os registros descritos no REQUISITO I.45.

2.1.10.3 Requisitos de Arquivamento de Chaves Privadas no Software de AC

RECOMENDAÇÃO I.09: Um Software de AC pode oferecer um serviço de arquivamento de chaves privadas de certificado digital de sigilo conforme DOC-ICP-04 [5].

Procedimentos de ensaio para NSH 1, 2 e 3:

EN.REC.I.09.01: Verificar se a documentação técnica do Software de AC inclui:
●Uma afirmação da PI informando que não suporta esta recomendação; ou
●uma descrição sobre o serviço de arquivamento de chaves privadas de certificado digital de sigilo conforme DOC-ICP-04 [5].

EN.REC.I.09.02: Se o Software de AC suporta esta recomendação, utilizar o Software de AC para emitir um certificado digital de sigilo e solicitar que a chave privada deste certificado digital emitido seja arquivada pelo serviço de arquivamento de chaves privadas de certificado digital de sigilo. Depois, acessar esse serviço novamente e verificar que a chave privada do certificado digital de sigilo emitido está corretamente arquivada.

EN.REC.I.09.03: Se o Software de AC suporta esta recomendação, utilizar o Software de AC para verificar se todas as condições constantes no DOC-ICP-04 [5] estão presentes no serviço de arquivamento de chaves privadas de certificado digital de sigilo.

REQUISITO I.46: O serviço de arquivamento de chaves privadas para certificados digitais ICP-Brasil de sigilo, caso presente em um Software de AC, deve utilizar algoritmos simétricos definidos no DOC-ICP-01.01 [4], e também deve oferecer como proteção um nível de segurança não inferior àquele definido para a chave original.

Procedimentos de ensaio para NSH 1, 2 e 3:

EN.I.46.01: Verificar se a documentação técnica do Software de AC inclui:
- Uma afirmação da PI informando que não suporta este serviço; ou
- uma descrição sobre o serviço de arquivamento de chaves privadas para certificados digitais ICP-Brasil de sigilo.

EN.I.46.02: Verificar se a documentação técnica do Software de AC descreve que o serviço de arquivamento de chaves privadas para certificados digitais ICP-Brasil de sigilo utiliza algoritmos simétricos definidos no DOC-ICP- 01.01 [4], e também oferece como proteção um nível de segurança não inferior àquele definido para a chave original.

EN.I.46.03: Se o Software de AC suporta o serviço de arquivamento de chaves privadas para certificados digitais ICP-Brasil de sigilo, utilizar o Software da AC para verificar se este utiliza os algoritmos simétricos definidos no DOC-ICP-01.01 [4].

Procedimentos de ensaio para NSH 2 e 3:

EN.I.46.04: Se o Software de AC suporta o serviço de arquivamento de chaves privadas para certificados digitais ICP-Brasil de sigilo,verificar no código-fonte do

Software de AC se este oferece como proteção um nível de segurança não inferior àquele definido para a chave original.

2.1.10.4 Requisitos de Interação do Software de AC com Hardware Seguro

REQUISITO I.47: Um Software de AC deve utilizar hardware seguro (MSC ou HSM) para executar os serviços de ICP que necessitem utilizar a chave privada da AC (por exemplo, assinar certificados digitais, assinar LCR's etc). O hardware seguro (MSC ou HSM) a ser utilizado pelo Software de AC deve estar de acordo com o DOC-ICP-01.01 [4].

Procedimentos de ensaio para NSH 1, 2 e 3:

EN.I.47.01: Verificar se a documentação técnica do Software de AC descreve sobre a utilização de hardware seguro (MSC ou HSM) para executar os serviços de ICP que necessitem utilizar a chave privada da AC.

EN.I.47.02: Verificar se a documentação técnica do Software de AC descreve que o hardware seguro (MSC ou HSM) está de acordo com o DOC-ICP-01.01 [4].

EN.I.47.03: Utilizar o Software da AC para verificar se o hardware seguro (MSC ou HSM) executa os serviços de ICP que necessitam da chave privada da AC (por exemplo, assinar certificados digitais, assinar LCR's etc).

EN.I.47.04: Utilizar o Software da AC para verificar se o hardware seguro (MSC ou HSM) está de acordo com o DOC-ICP-01.01 [4].

Procedimentos de ensaio para NSH 2 e 3:

EN.I.47.05: Verificar no código-fonte do Software de AC se um componente de PSC para interação do Software de AC e o hardware seguro (MSC ou HSM) possui mecanismos de segurança, tais como canal seguro, emissão e geração de chaves criptográficas etc.

OBSERVAÇÃO: A ICP-Brasil regulamenta no DOC-ICP-05 [7] que o processo de geração do par de chaves criptográficas assimétricas da AC deve ser feito por hardware seguro (MSC ou HSM) ou por software. A geração por software é admitida apenas para chaves de AC utilizadas exclusivamente para assinatura de certificados dos tipos A1 ou S1.

2.1.11 Requisitos de Documentação para Software de AC

REQUISITO I.48: Um Software de AC deve ter as seguintes documentações em idioma português do Brasil ou inglês:

- Manual de usuário;
- manual de instalação;
- documentos de especificação técnica.

Procedimentos de ensaio para NSH 1, 2 e 3:

EN.I.48.01: Verificar se a documentação técnica do Software de AC inclui o manual de usuário, o manual de instalação e os documentos de especificação técnica em idioma português do Brasil ou inglês.

REQUISITO I.49: Um Software de AC deve possuir a configuração da sua interface em idioma português do Brasil ou inglês.

Procedimentos de ensaio para NSH 1, 2 e 3:

EN.I.49.01: Verificar se a documentação técnica do Software de AC descreve sobre a configuração da sua interface.

EN.I.49.02: Acessar o Software de AC e verificar se a sua interface está em idioma português do Brasil ou inglês.

REQUISITO I.50: Um Software de AC deve possuir tópicos de ajuda em idioma português do Brasil ou inglês.

Procedimentos de ensaio para NSH 1, 2 e 3:

EN.I.50.01: Acessar o Software de AC e verificar se este possui tópicos de ajuda em idioma português do Brasil ou inglês.

REQUISITO I.51: O manual de usuário ou o manual de instalação ou os documentos de especificação técnica devem informar quais as plataformas de sistema operacional suportadas pelo Software de AC e quais os requisitos de ambiente operacional necessários para sua operação.

Procedimentos de ensaio para NSH 1, 2 e 3:

EN.I.51.01: Verificar se em um desses documentos (o manual de usuário ou o manual de instalação ou os documentos de especificação técnica) é informado quais as plataformas de sistema operacional suportadas pelo Software de AC e quais os requisitos de ambiente operacional necessários para sua operação.

REQUISITO I.52: Um Software de AC deve permitir ao operador ou administrador visualizar a versão do software e o nome de seu responsável.

Procedimentos de ensaio para NSH 1, 2 e 3:

EN.I.52.01: Acessar o Software de AC e verificar se este permite ao operador ou ao administrador visualizar a versão do software e o nome de seu responsável.

REQUISITO I.53: De acordo com item 6.6 do DOC-ICP-05 [7], um Software de AC deve possuir documentação das práticas de engenharia de software adotadas, metodologia de desenvolvimento de software, entre outros, aplicados ao Software de AC ou a qualquer outro software desenvolvido ou utilizado pela AC.

Procedimentos de ensaio para NSH 1, 2 e 3:

EN.I.53.01: Verificar se a documentação técnica do Software de AC inclui documentação das práticas de engenharia de software adotadas, metodologia de desenvolvimento de software, entre outros, aplicados ao Software de AC ou a qualquer outro software desenvolvido ou utilizado pela AC.

2.2 Requisitos aplicáveis somente ao Software de AR

Nesta seção estão definidos os requisitos aplicáveis apenas a um Software de AR.

2.2.1 Requisitos Gerais de um Software de AR

Conforme o glossário ICP-Brasil [8], uma AR é definida como uma entidade responsável pela interface entre o usuário e a AC. Sendo vinculada a uma AC, a AR tem por objetivo o recebimento, validação, encaminhamento de solicitações de emissão ou revogação de certificados digitais às AC e identificação, de forma presencial, de seus solicitantes. É responsabilidade da AR manter registros de suas operações. Pode estar fisicamente localizada em uma AC ou ser uma entidade de registro remota.
Portanto, um Software de AR deve prover funcionalidades que permitam a uma AR desempenhar seus objetivos conforme definidos no glossário ICP-Brasil [8].

REQUISITO II.01: Um Software de AR deve oferecer, no mínimo, as seguintes componentes e funcionalidades:

- Cadastrar usuários finais;
- receber, validar e encaminhar solicitações de emissão, revogação ou renovação de certificados digitais às AC´s;
- informar aos respectivos titulares a emissão ou revogação de seus certificados;
- gerar os registros de suas operações.

Procedimentos de ensaio para NSH 1, 2 e 3:

EN.II.01.01: Verificar se a documentação técnica do Software de AR descreve sobre os componentes e funcionalidades descritos no REQUISITO II.01.

EN.II.01.02: Utilizar o software da AR para verificar se este oferece todos os componentes e funcionalidades descritos no REQUISITO II.01.

Procedimentos de ensaio para NSH 2 e 3:

EN.II.01.03: Verificar no código-fonte do Software de AR as rotinas para executar todos os componentes e funcionalidades descritos no REQUISITO II.01. Depois, testar as execuções dessas rotinas.

2.2.2 Requisitos de Segurança

REQUISITO II.02: Um Software de AR deve possuir, no mínimo, as seguintes características de segurança:

1. Acesso permitido mediante autenticação por meio do certificado do Agente de Registro, no mínimo, do tipo A3;
2. acesso permitido somente a partir de equipamentos previamente autenticados ou cadastrados no Software de AR (ex. usando cadastramento prévio de endereço IP, ou outra solução que permita ao Software de AR autenticar o equipamento);
3. *timeout* de sessão;
4. registro de auditoria dos eventos citados no item 4.5.1 do DOC-ICP-05 [7];
5. histórico da inclusão e exclusão dos Agentes de Registro no sistema e das permissões concedidas ou revogadas;
6. registro informando se a validação da solicitação de certificados foi executada interna ou externamente ao ambiente da AR, para cada certificado digital emitido;
7. toda comunicação entre a AR e a AC e entre a AR e o usuário final deve ocorrer por meio de um canal seguro utilizando os padrões e algoritmos criptográficos da ICP-Brasil, conforme DOC-ICP-01.01 [4], que possibilitem o sigilo dos dados trafegados;

Procedimentos de ensaio para NSH 1, 2 e 3:

EN.II.02.01: Verificar se a documentação técnica do Software de AR descreve sobre as características de segurança descritas no REQUISITO II.02.

EN.II.02.02: Acessar o Software de AR por meio de um operador (Agente de Registro) previamente cadastrado pelo administrador do Software de AR. Fazer a autenticação com um certificado digital ICP-Brasil do tipo A1 ou A2 desse operador e verificar que esse acesso não será permitido. Depois, utilizar um certificado digital válido do tipo A3 ou A4 desse mesmo operador e conseguir o acesso ao Software de AR.

EN.II.02.03: Acessar o Software de AR por meio de um operador (Agente de Registro) previamente cadastrado pelo administrador do Software de AR. Fazer a autenticação usando uma leitora de cartões não cadastrada no ambiente operacional utilizado no ensaio e, mesmo que utilizando um certificado digital ICP-Brasil do tipo A3 do operador já cadastrado, verificar que o Software de AR não permitirá o acesso. Depois, utilizar uma leitora de cartões previamente cadastrada no Software de AR com o certificado digital ICP-Brasil do tipo A3 do operador já cadastrado e verificar que o acesso será permitido.

EN.II.02.04: Acessar o Software de AR por meio de um operador (Agente de Registro) previamente cadastrado pelo administrador do Software de AR. Após aguardar um período sem utilizar o Software de AR, verificar se ocorre o *logout* do software após o tempo decorrido de *timeout* (que foi previamente cadastrado nas configurações do Software de AR).

EN.II.02.05: Acessar o Software de AR e verificar se este possui, no mínimo, os registros de auditoria dos eventos citados no item 4.5.1 do DOC-ICP-05 [7].

EN.II.02.06: Acessar o Software de AR e verificar se este possui uma funcionalidade que mostre o histórico da inclusão e exclusão dos Agentes de Registro no sistema e das permissões concedidas ou revogadas.

EN.II.02.07: Acessar o Software de AR e verificar se este possui um registro para informar se a validação da solicitação de certificados foi executada interna ou externamente ao ambiente da AR, para cada certificado digital emitido.

EN.II.02.08: Acessar o Software de AR e o Software de AC para verificar, utilizando uma ferramenta especifica, se toda comunicação entre a AR e a AC e entre a AR e o usuário final ocorre por meio de um canal seguro, obedecendo aos padrões e algoritmos criptográficos da ICP-Brasil, conforme DOC-ICP-01.01 [4], que possibilitem o sigilo dos dados trafegados.

RECOMENDAÇÃO II.01: Um software de AR pode controlar a liberação de solicitação de certificados digitais por meio da autorização de dois ou mais agentes de registros.

Procedimentos de ensaio para NSH 1, 2 e 3:

EN.REC.II.01.01: Verificar se a documentação técnica do Software de AR inclui:
- Uma afirmação da PI informando que não suporta esta recomendação; ou
- uma descrição sobre o processo de liberação de solicitação de certificados digitais por meio da autorização de dois ou mais agentes de registros.

EN.REC.II.01.02: Se o Software de AR suporta esta recomendação, acessar o Software de AR por meio de um operador previamente cadastrado (Agente de Registro) e autorizar a emissão de um certificado digital previamente solicitado. Verificar que o Software de AR pede que somente outro Agente de Registro autorize a emissão deste certificado digital. Para tal, fazer o *logout* do primeiro operador de AR e acessar o Software de AR com outro operador de AR (Agente de Registro). Então, com o novo operador de AR, liberar a emissão do certificado digital e verificar que esta liberação foi autorizada.

2.2.2.1 Requisitos de Auditoria de Software de AR

REQUISITO II.03: Um Software de AR deve gerar, no mínimo, os seguintes registros para:

- Controle de acesso:
  - registros relacionados ao controle de acesso;
- autenticação:
  - registros relacionados às atividades de autenticação;
- atividades:
  - registros relacionados às atividades desempenhadas pela AR;
- banco de dados:
  - registros relacionados às atividades desempenhadas com o banco de dados;
- HTTP:
  - registros relacionados às atividades desempenhadas com o servidor web que interage com os usuários finais.

Procedimentos de ensaio para NSH 1, 2 e 3:

EN.II.03.01: Verificar se a documentação técnica do Software de AR descreve sobre os seus registros gerados.

EN.II.03.02: Verificar se a documentação técnica do Software de AR descreve sobre, no mínimo, os tipos de registros citados no REQUISITO II.03.

EN.II.03.03: Utilizar o Software de AR e verificar se este possui, no mínimo, os registros citados no REQUISITO II.03.

2.2.3 Requisitos de Documentação para Software de AR

REQUISITO II.04: Um Software de AR deve ter as seguintes documentações em idioma português do Brasil ou inglês:

- Manual de usuário;
- manual de instalação;
- documentos de especificação técnica.

Procedimentos de ensaio para NSH 1, 2 e 3:

EN.II.04.01: Verificar se a documentação técnica do Software de AR inclui o manual de usuário, o manual de instalação e os documentos de especificação técnica em idioma português do Brasil ou inglês.

REQUISITO II.05: Um Software de AR deve possuir a configuração da sua interface em idioma português do Brasil ou inglês.

Procedimentos de ensaio para NSH 1, 2 e 3:

EN.II.05.01: Verificar se a documentação técnica do Software de AR descreve sobre a configuração da sua interface.

EN.II.05.02: Acessar o Software de AR e verificar se a sua interface está em idioma português do Brasil ou inglês.

REQUISITO II.06: Um Software de AR deve possuir tópicos de ajuda em idioma português do Brasil ou inglês.

Procedimentos de ensaio para NSH 1, 2 e 3:

EN.II.06.01: Acessar o Software de AR e verificar se este possui tópicos de ajuda em idioma português do Brasil ou inglês.

REQUISITO II.07: O manual de usuário ou o manual de instalação ou os documentos de especificação técnica deve informar quais as plataformas de sistema operacional suportadas pelo Software de AR e quais os requisitos de ambiente operacional necessários para sua operação.

Procedimentos de ensaio para NSH 1, 2 e 3:

EN.II.07.01: Verificar se em um desses documentos (o manual de usuário ou o manual de instalação ou os documentos de especificação técnica) é informado

quais as plataformas de sistema operacional suportadas pelo Software de AR e quais os requisitos de ambiente operacional necessários para sua operação.

REQUISITO II.08: Um Software de AR deve permitir ao operador ou administrador visualizar a versão do software e o nome de seu responsável.

Procedimentos de ensaio para NSH 1, 2 e 3:

EN.II.08.01: Acessar o Software de AR e verificar se este permite ao operador ou ao administrador visualizar a versão do software e o nome de seu responsável.

REQUISITO II.09: De acordo com item 6.6 do DOC-ICP-05 [8], um Software de AR deve possuir documentação das práticas de engenharia de software adotadas, metodologia de desenvolvimento de software, entre outros, aplicados ao Software de AR ou a qualquer outro software desenvolvido ou utilizado pela AR.

Procedimentos de ensaio para NSH 1, 2 e 3:

EN.II.09.01: Verificar se a documentação técnica do Software de AR inclui documentação das práticas de engenharia de software adotadas, metodologia de desenvolvimento de software, entre outros, aplicados ao Software de AR ou a qualquer outro software desenvolvido ou utilizado pela AR.

2.3 Requisitos aplicáveis ao Software de AC e AR

Nesta seção são abordados os requisitos sobre os papéis de acesso no Software de AC e de AR.

2.3.1 Requisitos de Papéis de Acesso

Nesta seção são abordados os requisitos sobre os papéis de acesso no Software de AC e de AR.

REQUISITO III.01: Um Software de AC ou AR deve dispor de, no mínimo, dois papéis de acesso autenticados ao sistema da AC ou AR:

- Operador da AC ou AR: papel que realiza funções gerenciais e operacionais;
- administrador da AC ou AR: papel que configura a AC ou AR.

Procedimentos de ensaio para NSH 1, 2 e 3:

EN.III.01.01: Verificar se a documentação técnica do Software de AC descreve sobre os papéis de acesso autenticados (no mínimo, operador e administrador de AC) ao sistema da AC.

EN.III.01.02: Verificar se a documentação técnica do Software de AR descreve sobre os papéis de acesso autenticados (no mínimo, operador e administrador de AR) ao sistema da AR.

EN.III.01.03: Utilizar o Software de AC para verificar a permissão, no mínimo, dos papéis de administrador (que realiza configurações da AC) e operador (que realiza funções gerenciais e operacionais da AC) para se autenticar no Software de AC.

EN.III.01.04: Utilizar o Software de AR para verificar a permissão, no mínimo, dos papéis de administrador (que realiza configurações da AR) e operador (que realiza funções gerenciais e operacionais da AR) para se autenticar no Software de AR.

REQUISITO III.02: Um Software de AC ou AR deve tornar disponíveis interfaces de acordo com cada papel de acesso disponível, e possibilitar apenas o acesso aos seus serviços correspondentes. Portanto, com relação às interfaces, um Software de AC ou AR deve ter:

- Interface de usuário final;
- interface de operador;
- interface de administrador.

Procedimentos de ensaio para NSH 1, 2 e 3:

EN.III.02.01: Verificar se a documentação técnica do Software de AC descreve sobre as interfaces dos papéis de acesso (operador de AC, administrador de AC e usuário final) ao sistema da AC.

EN.III.02.02: Verificar se a documentação técnica do Software de AR descreve sobre as interfaces dos papéis de acesso (operador de AR, administrador de AR e usuário final) ao sistema da AR.

EN.III.02.03: Utilizar o Software de AC para verificar se este possui as interfaces de administrador, de operador e de usuário final. Depois, verificar se cada uma dessas interfaces permite realizar apenas os serviços cabíveis a cada um dos papéis correspondentes.

EN.III.02.04: Utilizar o Software de AR para verificar se este possui as interfaces de administrador, de operador e de usuário final. Depois, verificar se cada uma dessas interfaces permite realizar apenas os serviços cabíveis a cada um dos papéis correspondentes.

2.3.2 Requisitos de Segurança

Esta subseção descreve os requisitos relacionados com a segurança dos Softwares de AC e AR.

REQUISITO III.03: Um Software de AC ou AR não deve permitir que sejam criados operadores com nomes iguais. Especificamente no Software de AC devem existir políticas de senhas que permitam controlar, no mínimo, a criação de senhas fortes, o bloqueio por número de tentativas erradas de senhas, a troca periódica de senhas, o tamanho mínimo de senhas e regras de formação de senhas.

Procedimentos de ensaio para NSH 1, 2 e 3:

EN.III.03.01: Verificar se a documentação técnica do Software de AC descreve sobre o controle para não permitir nomes iguais aos operadores.

EN.III.03.02: Verificar se a documentação técnica do Software de AR descreve sobre o controle para não permitir nomes iguais aos operadores.

EN.III.03.03: Verificar se a documentação técnica do Software de AC descreve sobre a política de senhas e que contenha, no mínimo, informações sobre a criação de senhas fortes, o bloqueio por número de tentativas erradas de senhas, a troca periódica de senhas, o tamanho mínimo de senhas e regras de formação de senhas.

EN.III.03.04: Verificar se a documentação técnica do Software de AR descreve sobre a política de senhas e que contenha, no mínimo, informações sobre a criação de senhas fortes, o bloqueio por número de tentativas erradas de senhas, a troca periódica de senhas, o tamanho mínimo de senhas e regras de formação de senhas.

EN.III.03.05: Acessar o Software de AC por meio de um administrador de AC e tentar criar dois operadores com nomes iguais. Verificar que isso não será permitido pelo Software de AC.

EN.III.03.06: Acessar o Software de AR por meio de um administrador de AR e tentar criar dois operadores com nomes iguais. Verificar que isso não será permitido pelo Software de AR.

EN.III.03.07: Acessar o Software de AC por meio de um administrador de AC e, ao criar um novo operador de AC, verificar se o Software de AC possui política para a criação de senhas fortes, o controle de bloqueio por número de tentativas erradas de senhas, a obrigação de troca periódica de senhas, o controle para tamanho mínimo de senhas e regras de formação de senhas.

EN.III.03.08: Acessar o Software de AR por meio de um administrador de AR e, ao criar um novo operador de AR, verificar se o Software de AR possui política para a criação de senhas fortes, o controle de bloqueio por número de tentativas erradas

de senhas, a obrigação de troca periódica de senhas, o controle para tamanho mínimo de senhas e regras de formação de senhas.

REQUISITO III.04: Um Software de AC ou AR não deve permitir o acesso as suas funcionalidades quando ocorrer falhas na autenticação.

Procedimentos de ensaio para NSH 1, 2 e 3:

EN.III.04.01: Verificar se a documentação técnica do Software de AC descreve sobre o controle de acesso às funcionalidades quando ocorrem falhas na autenticação.

EN.III.04.02: Verificar se a documentação técnica do Software de AR descreve sobre o controle de acesso às funcionalidades quando ocorrem falhas na autenticação.

EN.III.04.03: Acessar o Software de AC por meio de um operador de AC provocando erro na autenticação. Depois, verificar se alguma funcionalidade do Software de AC é disponibilizado ao operador da AC.

EN.III.04.04: Acessar o Software de AR por meio de um operador de AR provocando erro na autenticação. Depois, verificar se alguma funcionalidade do Software de AR é disponibilizado ao operador da AR.

REQUISITO III.05: Um Software de AC ou AR deve exibir ao operador, após sua autenticação bem sucedida, informações sobre o último acesso realizado. Esse requisito presente no Software de AC ou AR tem como objetivo possibilitar ao operador alertar sobre possíveis acessos não autorizados que possam ter ocorrido com o seu papel.

Procedimentos de ensaio para NSH 1, 2 e 3:

EN.III.05.01: Verificar se a documentação técnica do Software de AC descreve sobre as informações exibidas ao operador de seu último acesso realizado.

EN.III.05.02: Verificar se a documentação técnica do Software de AR descreve sobre as informações exibidas ao operador de seu último acesso realizado.

EN.III.05.03: Acessar o Software de AC por meio de um operador de AC e verificar se são exibidas informações sobre o último acesso realizado.

EN.III.05.04: Acessar o Software de AR por meio de um operador de AR e verificar se são exibidas informações sobre o último acesso realizado.

REQUISITO III.06: Um Software de AC ou AR deve ter a opção para que o operador efetue o *logoff* quando for encerrar as suas atividades.

Procedimentos de ensaio para NSH 1, 2 e 3:

EN.III.06.01: Verificar se a documentação técnica do Software de AC descreve sobre o processo de *logoff* quando o operador for encerrar as suas atividades.

EN.III.06.02: Verificar se a documentação técnica do Software de AR descreve sobre o processo de *logoff* quando o operador for encerrar as suas atividades.

EN.III.06.03: Acessar o Software de AC por meio de um operador de AC e verificar se é possível realizar o *logoff* do operador.

EN.III.06.04: Acessar o Software de AR por meio de um operador de AR e verificar se é possível realizar o *logoff* do operador.

REQUISITO III.07: Um Software de AC ou AR deve possibilitar ao administrador a configuração de número de tentativas para bloqueio de acesso do operador.

Procedimentos de ensaio para NSH 1, 2 e 3:

EN.III.07.01: Verificar se a documentação técnica do Software de AC descreve sobre a configuração de número de tentativas para bloqueio de acesso do operador feita somente pelo administrador.

EN.III.07.02: Verificar se a documentação técnica do Software de AR descreve sobre a configuração de número de tentativas para bloqueio de acesso do operador feita somente pelo administrador.

EN.III.07.03: Acessar o Software de AC por meio de um operador de AC e tentar configurar o número de tentativas para bloqueio de acesso. Verificar que o Software de AC não aceita que esta configuração seja realizada por um operador.

EN.III.07.04: Acessar o Software de AR por meio de um operador de AR e tentar configurar o número de tentativas para bloqueio de acesso. Verificar que o Software de AR não aceita que esta configuração seja realizada por um operador.

REQUISITO III.08: Um Software de AC ou AR deve permitir que somente o administrador faça a criação, a alteração, a suspensão temporária, a exclusão e o desbloqueio do papel de acesso do operador.

Procedimentos de ensaio para NSH 1, 2 e 3:

EN.III.08.01: Verificar se a documentação técnica do Software de AC descreve sobre a criação, a alteração, a suspensão temporária, a exclusão e o desbloqueio do papel de acesso do operador feitos pelo administrador.

EN.III.08.02: Verificar se a documentação técnica do Software de AR descreve sobre a criação, a alteração, a suspensão temporária, a exclusão e o desbloqueio do papel de acesso do operador feitos pelo administrador.

EN.III.08.03: Acessar o Software de AC por meio de um operador de AC e tentar criar, alterar, suspender temporariamente, excluir e desbloquear o acesso de um

operador de AC. Verificar que o Software de AC não aceita que estas operações sejam realizadas por um operador.

EN.III.08.04: Acessar o Software de AR por meio de um operador de AR e tentar criar, alterar, suspender temporariamente, excluir e desbloquear o acesso de um operador de AR. Verificar que o Software de AR não aceita que estas operações sejam realizadas por um operador.

REQUISITO III.09: Um Software de AC ou AR deve possibilitar a configuração de parâmetros de *timeout* para os casos de inatividade da sessão.

Procedimentos de ensaio para NSH 1, 2 e 3:

EN.III.09.01: Verificar se a documentação técnica do Software de AC descreve sobre a configuração de parâmetros de *timeout* para os casos de inatividade da sessão.

EN.III.09.02: Verificar se a documentação técnica do Software de AR descreve sobre a configuração de parâmetros de *timeout* para os casos de inatividade da sessão.

EN.III.09.03: Verificar se o Software de AC possui uma opção de configuração de parâmetros de *timeout* para os casos de inatividade da sessão. Depois de configurar esses parâmetros, verificar se ocorre a inatividade da sessão em função dos parâmetros de *timeout* anteriormente configurados.

EN.III.09.04: Verificar se o Software de AR possui uma opção de configuração de parâmetros de *timeout* para os casos de inatividade da sessão. Depois de configurar esses parâmetros, verificar se ocorre a inatividade da sessão em função dos parâmetros de *timeout* anteriormente configurados.

REQUISITO III.10: Um Software de AC ou AR não deve permitir que sejam efetuadas quaisquer operações após o tempo de *timeout* decorrido.

Procedimentos de ensaio para NSH 1, 2 e 3:

EN.III.10.01: Verificar se a documentação técnica do Software de AC descreve sobre o fato de não permitir que sejam efetuadas quaisquer operações após o tempo de *timeout* decorrido.

EN.III.10.02: Verificar se a documentação técnica do Software de AR descreve sobre o fato de não permitir que sejam efetuadas quaisquer operações após o tempo de *timeout* decorrido.

EN.III.10.03: Acessar o Software de AC com o *login* de um operador de AC e aguardar para que o software encerre após o *timeout* decorrido. Depois, tentar executar alguma operação no Software de AC e verificar que isso não será mais possível.

EN.III.10.04: Acessar o Software de AR com o certificado digital A3 de um operador de AR e aguardar para que o software encerre após o *timeout* decorrido. Depois, tentar executar alguma operação no Software de AR e verificar que isso não será mais possível.

REQUISITO III.11: Um Software de AC ou AR deve solicitar que o operador efetue novo *login* após sua sessão ter sido encerrada devido à inatividade.

Procedimentos de ensaio para NSH 1, 2 e 3:

EN.III.11.01: Verificar se a documentação técnica do Software de AC descreve sobre o fato de o operador ter que efetuar novo *login* após sua sessão ter sido encerrada devido à inatividade.

EN.III.11.02: Verificar se a documentação técnica do Software de AR descreve sobre o fato de o operador ter que efetuar novo *login* após sua sessão ter sido encerrada devido à inatividade.

EN.III.11.03: Acessar o Software de AC com o *login* de um operador de AC e aguardar para que o software encerre após a inatividade. Depois, verificar que o Software de AC solicitará que seja feito um novo acesso.

EN.III.11.04: Acessar o Software de AR com o certificado digital A3 de um operador de AR e aguardar para que o software encerre após a inatividade. Depois, verificar que o Software de AR solicitará que seja feito novo acesso.

RECOMENDAÇÃO III.01: Um Software de AC ou AR pode permitir o gerenciamento de perfil por grupos de usuários (operadores e/ou administradores).

Procedimentos de ensaio para NSH 1, 2 e 3:

EN.REC.III.01.01: Verificar se a documentação técnica do Software de AC inclui:
- Uma afirmação da PI informando que não suporta esta recomendação; ou
- uma descrição sobre o gerenciamento de perfil por grupos de usuários (operadores e/ou administradores).

EN.REC.III.01.02: Verificar se a documentação técnica do Software de AR inclui:
- Uma afirmação da PI informando que não suporta esta recomendação; ou
- uma descrição sobre o gerenciamento de perfil por grupos de usuários (operadores e/ou administradores).

EN.REC.III.01.03: Se o Software de AC suporta esta recomendação, gerar grupos de usuários (operadores e/ou administradores de AC) e verificar se as autenticações utilizando esses grupos gerados são realizadas com sucesso.

EN.REC.III.01.04: Se o Software de AR suporta esta recomendação, gerar grupos de usuários (operadores e/ou administradores de AR) e verificar se as autenticações utilizando esses grupos gerados são realizadas com sucesso.

2.3.2.1 Requisitos de Auditoria de Software de AC ou AR

REQUISITO III.12: Um Software de AC ou AR deve gerar registros para finalidades de auditoria de acordo com a seção 4.5 do DOC-ICP-05 [7].

Procedimentos de ensaio para NSH 1, 2 e 3:

EN.III.12.01: Verificar se a documentação técnica do Software de AC descreve sobre os registros para finalidades de auditoria e que estejam de acordo com a seção 4.5 do DOC-ICP-05 [7].

EN.III.12.02: Verificar se a documentação técnica do Software de AR descreve sobre os registros para finalidades de auditoria e que estejam de acordo com a seção 4.5 do DOC-ICP-05 [7].

EN.III.12.03: Acessar o Software de AC para verificar se os registros gerados para finalidades de auditoria estão de acordo com a seção 4.5 do DOC-ICP-05 [7].

EN.III.12.04: Acessar o Software de AC para verificar se os registros gerados para finalidades de auditoria estão de acordo com a seção 4.5 do DOC-ICP-05 [7].

REQUISITO III.13: Um Software de AC ou AR deve prever regras para a rotação dos registros (*log*) baseado em tempo ou tamanho dos registros.

Procedimentos de ensaio para NSH 1, 2 e 3:

EN.III.13.01: Verificar se a documentação técnica do Software de AC descreve sobre as regras para a rotação dos registros (*log*) baseado em tempo ou tamanho dos registros.

EN.III.13.02: Verificar se a documentação técnica do Software de AR descreve sobre as regras para a rotação dos registros (*log*) baseado em tempo ou tamanho dos registros.

EN.III.13.03: Verificar se o Software de AC possui a funcionalidade de rotação dos seus registros (*log*) baseado em tempo ou no tamanho dos registros.

EN.III.13.04: Verificar se o Software de AR possui a funcionalidade de rotação dos seus registros (*log*) baseado em tempo ou no tamanho dos registros.

RECOMENDAÇÃO III.02: Um Software de AC ou AR pode ter a opção de assinar digitalmente os seus registros gerados.

Procedimentos de ensaio para NSH 1, 2 e 3:

EN.REC.III.02.01: Verificar se a documentação técnica do Software de AC inclui:
- Uma afirmação da PI informando que não suporta esta recomendação; ou
- uma descrição sobre o processo de assinatura digital dos seus registros gerados.

EN.REC.III.02.02: Verificar se a documentação técnica do Software de AR inclui:
- Uma afirmação da PI informando que não suporta esta recomendação; ou
- uma descrição sobre o processo de assinatura digital dos seus registros gerados.

EN.REC.III.02.03: Se o Software de AC suporta esta recomendação, utilizar uma ferramenta especifica para verificar se os registros gerados pelo software são assinados digitalmente.

EN.REC.III.02.04: Se o Software de AR suporta esta recomendação, utilizar uma ferramenta especifica para verificar se os registros gerados pelo software são assinados digitalmente.

Referências Normativas

[1] COMITÊ GESTOR DA ICP-BRASIL. **Resolução N° 49, de 03 de Junho de 2008: Declaração de Práticas de Certificação da AC Raiz da ICP-Brasil.** Brasília. ICP-BRASIL, 2008. 23 p.

[2] COMITÊ GESTOR DA ICP-BRASIL. **Resolução N° 41, de 18 de abril de 2006: Requisitos Mínimos para as Políticas de Certificados na Infraestrutura de Chaves Públicas Brasileira (ICP-BRASIL).** Brasília. ICP-BRASIL, 2006. 20 p.

[3] COMITÊ GESTOR DA ICP-BRASIL. **DOC-ICP-01: Declaração de Práticas de Certificação da Autoridade Certificadora Raiz da ICP-Brasil.** versão 4.0. Brasília. ICP-BRASIL. 2008.

[4] COMITÊ GESTOR DA ICP-BRASIL. **DOC-ICP-01.01: Padrões e Algoritmos Criptográficos da ICP-Brasil.** versão 1.1. Brasília. ICP-BRASIL. 2008.

[5] COMITÊ GESTOR DA ICP-BRASIL. **DOC-ICP-04: Requisitos Mínimos para as Políticas de Certificado na ICP-Brasil.** versão 3.0. Brasília. ICP-BRASIL. 2008.

[6] COMITÊ GESTOR DA ICP-BRASIL. **DOC-ICP-04.01: Atribuição de OID na ICP-Brasil.** versão 2.0. Brasília. ICP-BRASIL. 2009.

[7] COMITÊ GESTOR DA ICP-BRASIL. **DOC-ICP-05: Requisitos Mínimos para as Declarações de Práticas de Certificação das Autoridades Certificadoras da ICP-Brasil.** versão 3.1. Brasília. ICP-BRASIL. 2009.

[8] COMITÊ GESTOR DA ICP-BRASIL **GLOSSÁRIO ICP-BR – INFRA-ESTRUTURA DE CHAVES PÚBLICAS BRASILEIRAS. Glossário ICP-Brasil.** Versão 1.2. Brasília. ICP-BRASIL: 2007.

[9] INTERNATIONAL ORGANIZATION FOR STANDARDIZATION / INTERNATIONAL ELECTROTECHNICAL COMMISSION. **Information technology - ASN.1 encoding rules: Specification of Basic Encoding Rules (BER), Canonical Encoding Rules (CER) and Distinguished Encoding Rules (DER) – ISO/IEC 8825-1.** Switzerland. ISO/IEC 8825-1:2002.

[10] RSA LABORATORIES. **PKCS#7. Cryptographic Message Syntax Standard.** version 1.5. 1993. 30p. Disponível em: <ftp://ftp.rsasecurity.com/pub/pkcs/doc/pkcs-7.doc>. Acesso em: 30.set.2009.

[11] RSA LABORATORIES **PKCS#10: Certification Request Syntax Standard.** Version 1.7. 2000. Disponível em: <ftp://ftp.rsasecurity.com/pub/pkcs/pkcs-10/pkcs-10v1_7.pdf>. Acesso em: 05.out.2009.

[12] THE INTERNET ENGINEERING TASK FORCE. Linn, J. **Privacy Enhancement for Internet Electronic Mail. Part I: Message Encryption and Authentication Procedures. RFC 1421.** 1993. Disponível em: <http://www.ietf.org/rfc/rfc1421.txt>. Acesso em: 30.set.2009.

[13] THE INTERNET ENGINEERING TASK FORCE. D. Cooper, S. Santesson, S. Farrell, S. Boeyen, R. Housley, W. Polk **Internet X.509 Public Key Infrastructure - Certificate and Certificate Revocation List (CRL) Profile. RFC 5280**, Category: Standards Track. 2008. Disponível em <http://www.ietf.org/rfc/rfc5280.txt>. Acesso em: 10.set.2009.

[14] THE INTERNET ENGINEERING TASK FORCE. Myers, M.; Ankney, R.; Malpani, A.; Galperin, S. e Adams, C. **X.509 Internet Public Key Infrastructure Online Certificate Status Protocol - OCSP. RFC 2560**, Category: Standards Track. 1999. Disponível em <http://www.ietf.org/rfc/rfc2560.txt>. Acesso em: 10.set.2009.

[15] THE INTERNET ENGINEERING TASK FORCE. Housley, R. **Cryptographic Message Syntax (CMS). RFC 3852**, Category: Standards Track. 2004. Disponível em <http://www.ietf.org/rfc/rfc3852.txt>. Acesso em: 30.set.2009.

[16] THE INTERNET ENGINEERING TASK FORCE. Housley, R.; Polk, W.; Ford, W. e Solo, D. **Internet X.509 Public Key Infrastructure - Certificate and Certificate Revocation List (CRL) Profile. RFC 3280**, Category: Standards Track, April 2002. Disponível em <http://www.ietf.org/rfc/rfc3280.txt>. Acesso em: 20.set.2009.

[17] THE INTERNET ENGINEERING TASK FORCE. S. Josefsson. **The Base16, Base32, and Base64 Data Encodings. RFC 4648,** Category: Standards Track. 2006. Disponível em <http://www.rfc-editor.org/rfc/rfc4648.txt>. Acesso em: 07.out.2009.

[18] AMERICAN NATIONAL STANDARDS INSTITUTE. **Digital Signatures Using Reversible Public Key Cryptography for the Financial Services Industry (rDSA). ANSI. X9.31.**1998.